INCIDENT RESPONSE STANDARD

Standard Title:	**INCIDENT RESPONSE STANDARD (NSU-IR)**
Standard Number:	**38-10.8**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**INCIDENT RESPONSE (IR)**
Approval Date:	**10/21/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all university information technology and data, whether owned and operated by the university, or used for university business through contractual arrangements.

STANDARD STATEMENT

All individuals to whom this standard applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university, or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS PAGE NUMBER

STANDARD STATEMENT 1
DEFINITIONS 1
CONTACT(S) 3
STAKEHOLDER(S) 3
INCIDENT RESPONSE (IR) 4
EDUCATION AND COMPLIANCE 6
EXCEPTIONS 7
REVIEW SCHEDULE 7
RELATED DOCUMENTS 7

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Availability: The property that data or information is accessible and usable upon demand by an authorized person and that timely, reliable access to data and information services is provided for authorized users.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidentiality: Protection of systems and data so that unauthorized parties cannot view the data, the property that sensitive information is not disclosed to unauthorized entities, and the assurance that information is not disclosed to unauthorized individuals or processes.

Controlled Unclassified Information (CUI): Information the Federal government owns or has created that needs to be safeguarded and disseminated using only controls consistent with Federal laws, regulations and policies.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of university data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property: Please refer to the BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)

The Office of Information Technology (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

STAKEHOLDER(S)

University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

INCIDENT RESPONSE (IR)

NSU-IR-1 INCIDENT RESPONSE TRAINING

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within 30 days of assuming an incident response role or responsibility or acquiring system access;
   2. When required by system changes; and
   3. Annually thereafter;
b. Review and update incident response training content on an annual basis and following environmental change or security incident;
c. Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations; and
d. Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

NSU-IR-2 INCIDENT RESPONSE TESTING

a. Test the effectiveness of the incident response capability for the system on an annual basis and following an environmental change using organization-defined tests;
b. Coordinate incident response testing with organizational elements responsible for related plans; and
c. Use qualitative and quantitative data from testing to:
   1. Determine the effectiveness of incident response processes;
   2. Continuously improve incident response processes; and
   3. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

NSU-IR-3 INCIDENT HANDLING

a. Implement an incident handling capability for security incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly;
d. Support the incident handling process using automated mechanisms where applicable;
e. Identify organization-defined classes of incidents and take actions in response to those incidents to ensure continuation of organizational mission and business functions;
f. Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response;

g. Implement a configurable capability to automatically disable the system if organization-defined security violations are detected;
h. Implement an incident handling capability for incidents involving insider threats;
i. Establish and maintain an integrated incident response team that can be deployed to any location on campus within a reasonable timeframe commensurate with the incident;
j. Analyze malicious code and/or other residual artifacts remaining in the system after the incident;
k. Analyze anomalous or suspected adversarial behavior in or related to organization environments and resources; and
l. Establish and maintain a security operations center.

NSU-IR-4 INCIDENT MONITORING

a. Track and document incidents; and
b. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

NSU-IR-5 INCIDENT REPORTING

a. Require personnel to report suspected incidents to the organizational incident response capability within 24 hours from when the University discovered or should have discovered their occurrence; and
b. Report incident information to the Chief Information Security Officer.

NSU-IR-6 INCIDENT RESPONSE ASSISTANCE

a. Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

NSU-IR-7 INCIDENT RESPONSE PLAN

a. Develop an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization for incidents classified as S3 or higher;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;
9. Is reviewed and approved by the Agency Head or designee and the Chief Information Security Officer annually; and
10. Explicitly designates responsibility for incident response to the Chief Information Security Officer and designees.

b. Distribute copies of the incident response plan to the incident response personnel (identified by name and/or by role);
c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicate incident response plan changes to the incident response personnel (identified by name and/or by role); and
e. Protect the incident response plan from unauthorized disclosure and modification.

NSU-IR-8 INTRUSION PREVENTION

The University Shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:

a. Designate an individual responsible for the threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
b. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
c. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.

NSU-IR-9 SERVICE PROVIDERS

a. The University shall require that its service providers implement incident handling practices commensurate with that of the University's.

EDUCATION AND COMPLIANCE

This standard shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the standard in writing, electronic or otherwise, to the University community within 30 days of approval;
- Post the standard on the appropriate website; and
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

The Chief Information Security Officer (or designee) is responsible for official interpretation of this standard. Questions regarding the application of this standard should be directed to the Office of Information Technology. The Chief Information Security Officer reserves the right to revise or eliminate this standard.

Violations of this standard, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to

comply with requirements of this standard may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this standard must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: 10/21/2027
- Approval by, date: OIT Standards Development Group, 10/21/2024
- Revision History: 10/21/2024,10/27/2025,10/19/2026
- Supersedes: SEC530 Controls

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx
32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx
38-10 - Information Security Policy
https://www.nsu.edu/policy/bov-38-10.aspx